

10/521624

PATENT

450100-05082

DT09 Rec'd PCT/PTO 14 JAN 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Tatsuya IGARASHI et al.

International Application No.: PCT/JP2004/004919

International Filing Date: April 5, 2004

For: INFORMATION PROCESSING APPARATUS, ACCESS
CONTROL PROCESSING METHOD AND COMPUTER
PROGRAM

745 Fifth Avenue
New York, NY 10151

EXPRESS MAIL

Mailing Label Number: EV206809848US

Date of Deposit: January 14, 2005

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Barnet Schindler
(Typed or printed name of person mailing paper or fee)

Barnet Schindler
(Signature of person mailing paper or fee)

CLAIM OF PRIORITY UNDER 37 C.F.R. § 1.78(a)(2)

Mail Stop PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 35 U.S.C. 119, this application is entitled to a claim of priority to Japan
Application No. 2003-138552 filed 16 May 2003.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: William S. Frommer
William S. Frommer
Reg. No. 25,506
Tel. (212) 588-0800

10/521624

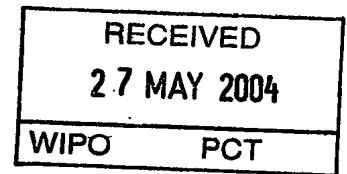
PCT/JP 2004/004919
Rec'd PCT/PTO 14 JAN 2005
05.4.2004日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 5 月 1 6 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 3 8 5 5 2
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 1 3 8 5 5 2]



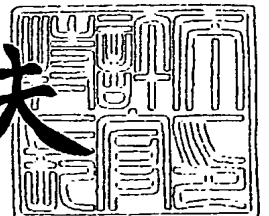
出 願 人 ソニー株式会社
Applicant(s):

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2 0 0 4 年 5 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 4 0 2 0 2

【書類名】 特許願

【整理番号】 0390214103

【提出日】 平成15年 5月16日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/32

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 五十嵐 卓也

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 吉川 典史

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 小堀 洋一

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 森田 岳彦

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 本田 康晃

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 田中 浩一

【特許出願人】

【識別番号】 000002185
【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100093241
【弁理士】
【氏名又は名称】 宮田 正昭
【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100101801
【弁理士】
【氏名又は名称】 山田 英治
【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531
【弁理士】
【氏名又は名称】 澤田 俊夫
【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 048747
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項 1】

アクセス制御処理を実行する情報処理装置であり、

マニュアル登録のなされたクライアントMACアドレスと、自動登録処理のなされたクライアントMACアドレスとを識別可能な態様で登録したMACアドレステーブルを記憶した記憶部と、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかに応じて、クライアントからのアクセス要求に対して異なるアクセス制御処理を実行するアクセス制御部とを有し、

前記アクセス制御部は、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、前記MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

情報処理装置に設定されたアクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、前記MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成を有することを特徴とする情報処理装置。

【請求項 2】

前記アクセス制御部は、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのMACアドレスを、前記MACアドレステーブルの規定登録限度

数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許可する処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項3】

前記アクセス制御を実行すべき要求種別は、

H T T P (Hyper Text Transfer Protocol)－G E Tメソッドに基づくコンテンツ要求処理、またはS O A P (Simple Object Access Protocol) に基づく制御要求処理の少なくともいずれかを含むことを特徴とする請求項2に記載の情報処理装置。

【請求項4】

前記情報処理装置は、

予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、クライアントMACアドレスを前記MACアドレステーブルにマニュアル登録のなされたクライアントMACアドレスとして登録する処理を実行する登録処理部を有することを特徴とする請求項1に記載の情報処理装置。

【請求項5】

前記情報処理装置は、

前記MACアドレステーブルに自動登録のなされたクライアントMACアドレスとして登録されたMACアドレスについて、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記MACアドレステーブルの自動登録クライアントMACアドレスエントリをマニュアル登録クライアントMACアドレスエントリとする設定変更処理を実行する登録処理部を有することを特徴とする請求項1に記載の情報処理装置。

【請求項6】

情報処理装置におけるアクセス制御処理方法であり、

クライアントからのアクセス要求を受信するアクセス要求受信ステップと、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ス

テップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、前記MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセス制御ステップと、

を有することを特徴とするアクセス制御処理方法。

【請求項 7】

前記アクセス制御ステップは、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのMACアドレスを、前記MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容する処理を実行することを特徴とする請求項 6 に記載のアクセス制御処理方法。

【請求項 8】

前記アクセス制御を実行すべき要求種別は、.....

HTTP (Hyper Text Transfer Protocol) - GET メソッドに基づくコンテンツ要求処理、または SOAP (Simple Object Access Protocol) に基づく制御要求処理の少なくともいずれかを含むことを特徴とする請求項 7 に記載のアクセス制御処理方法。

【請求項 9】

前記アクセス制御処理方法は、さらに、

予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処

理が実行されたことを条件として、クライアントMACアドレスを前記MACアドレステーブルにマニュアル登録のなされたクライアントMACアドレスとして登録する処理を実行する登録処理ステップを有することを特徴とする請求項6に記載のアクセス制御処理方法。

【請求項10】

前記アクセス制御処理方法は、さらに、

前記MACアドレステーブルに自動登録のなされたクライアントMACアドレスとして登録されたMACアドレスについて、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記MACアドレステーブルの自動登録クライアントMACアドレスエントリをマニュアル登録クライアントMACアドレスエントリとする設定変更処理を実行する登録処理ステップを有することを特徴とする請求項6に記載のアクセス制御処理方法。

【請求項11】

情報処理装置におけるアクセス制御処理を実行するコンピュータ・プログラムであり、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ステップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、前記MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセス制御ステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、ネットワーク接続された機器間の通信においてアクセス権限判定に基づくアクセス制御処理を実行する情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムに関する。

【0002】**【従来の技術】**

昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

【0003】

このようなホームネットワークの構成に適するプロトコルとしてユニバーサルプラグアンドプレイ (UPnP: Universal Plug and Play) が知られている。ユニバーサルプラグアンドプレイ (UPnP) は、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、困難な操作や設定を伴うことなくネットワーク接続された機器において各接続機器の提供サービスを受領可能とするものである。また、UPnPはデバイス上のOS (オペレーティングシステム) にも依存せず、容易に機器の追加ができるという利点を持つ。

【0004】

UPnPは、接続機器間で、XML (eXtensible Markup Language) に準拠した定義ファイルを交換し、機器間において相互認識を行なう。UPnPの処理の概要は、以下の通りである。

- (1) IPアドレス等の自己のデバイスIDを取得するアドレッシング処理。
- (2) ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受

信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

(3) ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

【0005】

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供および受領が可能となる。ネットワークに新たに接続される機器は、上記のアドレッシング処理によりデバイスIDを取得し、ディスカバリ処理によりネットワーク接続された他のデバイスの情報を取得して、取得情報に基づいて他の機器にサービスの要求が可能となる。

【0006】

しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホームネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。

【0007】

このようなホームネットワーク内のサーバに格納されたコンテンツは、ネットワーク接続された他の機器からアクセス可能となる。例えば、上述の簡易な機器接続構成であるUPnP接続を実行した機器によってコンテンツを取得することが可能となる。コンテンツが映画データや音楽データの場合、ネットワーク接続機器としてTV、あるいはプレーヤ等を接続すれば、映画を視聴したり、音楽を聴いたりすることが可能となる。

【0008】

コンテンツの利用権を有するユーザの接続した機器によるアクセスは許容されてもよいが、上述のようなネットワーク構成においては、コンテンツ等の利用権を持たないユーザがネットワークに入り込むことも容易である。例えば無線LANによって構成されたネットワークの場合には家の中にあるサーバに対して、戸外、あるいは隣家等から通信機器を利用して不正にネットワークに参入し、コンテンツの搾取を行なうような事態も発生し得る。このような不正なアクセスを許

容する構成は、秘密漏洩を生じさせることにもなり、また、コンテンツ著作権の管理の観点からも重要な問題となる。

【0009】

上述のような不正アクセスを排除するため、例えばサーバにアクセスを許容するクライアントのリストを保持させ、クライアントからサーバに対するアクセス要求の際に、サーバでリストとの照合処理を実行して不正アクセスを排除する構成が提案されている。

【0010】

例えば、ネットワーク接続機器に固有の物理アドレスであるMAC (Media Access Control) アドレスを、アクセス許容機器リストとして設定するMACアドレスフィルタリングが知られている。MACアドレスフィルタリングとは、ホームネットワーク等の内部ネットワーク（サブネット）と外部ネットワークとを隔離するルータあるいはゲートウェイに、予めアクセスを許容するMACアドレスを登録しておき、受信したパケットのMACアドレスと登録されたMACアドレスとを照合し、登録されていないMACアドレスを有する機器からのアクセスを拒否するものである。なお、この種の技術については、例えば特許文献1に開示されている。

【0011】

しかし、一般にアクセス制限をするためのMACアドレスの登録処理を行なうためには、ユーザあるいは管理者がネットワークに接続される機器のMACアドレスを調べて、調べたMACアドレスをオペレータが入力してリストを作成するという処理が必要となる。

【0012】

ホームネットワークにおいては、新たな機器の追加処理が行われることは頻繁に発生することであり、このような機器追加処理の際に、ユーザが逐次、機器のMACアドレスを調べて登録処理をしなければならないとすると、ネットワーク構築の容易性を阻害することになる。

【0013】

一方、一般家庭においても、PCのみならず、家電機器も含んだネットワーク

構成が構築され、どのような機器からでもネットワークにアクセス可能ないわゆるユビキタス環境が構築されつつあり、また、無線LAN等の普及により、通信可能な機器が外部から無線LANに侵入することも容易となっている。このようなネットワーク環境において、ネットワーク接続機器に対する不正アクセスもより発生しやすくなっており、不正なアクセスによる秘密情報の搾取、コンテンツの不正読み取り等が実行される可能性はますます高くなっている。このような状況において、一般ユーザに負担を強いることなく、適切なアクセス制御構成を容易に実現することが求められている。

【0014】

【特許文献1】

特開平10-271154号公報

【0015】

【発明が解決しようとする課題】

本発明は、上述の問題点に鑑みてなされたものであり、様々な機器からのアクセス要求をネットワークを介して受領する情報処理装置におけるアクセス制御において、複数のモードに基づく異なる態様でのアクセス制御処理を可能とすることで、ユーザ負担の軽減を図るとともに、不特定多数クライアントからの無制限なアクセスについても防止可能とした情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0016】

【課題を解決するための手段】

本発明の第1の側面は、

アクセス制御処理を実行する情報処理装置であり、

マニュアル登録のなされたクライアントMACアドレスと、自動登録処理のなされたクライアントMACアドレスとを識別可能な態様で登録したMACアドレステーブルを記憶した記憶部と、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかに応じて、クライアントからのアクセス要求に対して異なるアクセス制御処理を実行するアクセス制御部

とを有し、

前記アクセス制御部は、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、前記MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

情報処理装置に設定されたアクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、前記MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成を有することを特徴とする情報処理装置にある。

【0017】

さらに、本発明の情報処理装置の一実施態様において、前記アクセス制御部は、情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのMACアドレスを、前記MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容する処理を実行する構成であることを特徴とする。

【0018】

さらに、本発明の情報処理装置の一実施態様において、前記アクセス制御を実行すべき要求種別は、H-T-T-P (Hyper Text Transfer Protocol) - G-E-T-メソッドに基づくコンテンツ要求処理、またはS-O-A-P (Simple Object Access Protocol) に基づく制御要求処理の少なくともいずれかを含むことを特徴とする。

【0019】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、クライアントMACアドレスを前記MACアドレステーブルにマニュアル登録のなされたクライアントMACアドレスとして登

録する処理を実行する登録処理部を有することを特徴とする。

【0020】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記MACアドレステーブルに自動登録のなされたクライアントMACアドレスとして登録されたMACアドレスについて、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記MACアドレステーブルの自動登録クライアントMACアドレスエントリをマニュアル登録クライアントMACアドレスエントリとする設定変更処理を実行する登録処理部を有することを特徴とする。

【0021】

さらに、本発明の第2の側面は、
情報処理装置におけるアクセス制御処理方法であり、
クライアントからのアクセス要求を受信するアクセス要求受信ステップと、
情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ステップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、前記MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセス制御ステップと、

を有することを特徴とするアクセス制御処理方法にある。

【0022】

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御ステップは、情報処理装置に設定されたアクセス制御モードが、自動登録ア

アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのMACアドレスを、前記MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容する処理を実行することを特徴とする。

【0023】

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御を実行すべき要求種別は、HTTP (Hyper Text Transfer Protocol) - GETメソッドなどに基づくコンテンツ要求処理、またはSOAP (Simple Object Access Protocol) に基づく制御要求処理の少なくともいずれかを含むことを特徴とする。

【0024】

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御処理方法は、さらに、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、クライアントMACアドレスを前記MACアドレステーブルにマニュアル登録のなされたクライアントMACアドレスとして登録する処理を実行する登録処理ステップを有することを特徴とする。

【0025】

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御処理方法は、さらに、前記MACアドレステーブルに自動登録のなされたクライアントMACアドレスとして登録されたMACアドレスについて、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記MACアドレステーブルの自動登録クライアントMACアドレスエントリをマニュアル登録クライアントMACアドレスエントリとする設定変更処理を実行する登録処理ステップを有することを特徴とする。

【0026】

さらに、本発明の第3の側面は、
情報処理装置におけるアクセス制御処理を実行するコンピュータ・プログラム

であり、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ステップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、前記MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセス制御ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【0027】

【作用】

本発明の構成においては、マニュアル登録のなされたクライアントMACアドレスと、自動登録処理のなされたクライアントMACアドレスとを識別可能な態様で登録したMACアドレステーブルを設定し、アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成としたので、ユーザによるマニュアル登録処理を実行しない場合においても、無制限なアクセスが防止され、例えば不特定多数クライアントからのサーバ格納コンテンツの取得等を防止することが可能となり、さらに、モードを、登録デバイスアクセス制御モー

ドに設定することにより、厳格なアクセス制御を実行することも可能となる。

【0028】

さらに、本発明の構成によれば、自動登録アクセス制御モードにおいて、クライアントのアクセス要求種別を識別し、識別されたアクセス要求種別が予め定められたアクセス制御を実行すべき要求種別、例えばHTTP (Hyper Text Transfer Protocol) - GETメソッドに基づくコンテンツ要求処理、またはSOAP (Simple Object Access Protocol) に基づく制御要求処理である場合にのみ、クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としたアクセス許可を実行する構成としたので、UPnP等における機器発見処理、情報取得処理等において不必要なアクセス制御を行うことが防止される。

【0029】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0030】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0031】

【発明の実施の形態】

以下、図面を参照しながら、本発明の情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムの詳細について説明する。

【0032】

[システム概要およびMACアドレステーブル]

まず、図1を参照して、本発明の適用可能なネットワーク構成例について説明する。図1は、様々なクライアント機器からの処理要求に応じて処理を実行するサーバ101と、サーバ101に対して処理要求を行なうクライアント機器としてのPC121、122、124、PDA、携帯電話等の携帯通信端末123、125がネットワーク100を介して接続された構成、例えばホームネットワーク構成を示している。

【0033】

サーバ101がクライアントからの要求に応じて実行する処理は、例えばサーバ101の保有するハードディスク等の記憶手段に格納されたコンテンツの提供、あるいはサーバの実行可能なアプリケーションプログラムの実行によるデータ処理サービス等である。なお、図1においては、サーバ101と、その他のクライアント機器としてのPC121、122、124、PDA、携帯電話等の携帯通信端末123、125とを区別して示しているが、クライアントからの要求に対するサービスを提供する機器をサーバとして示しているものであり、いずれのクライアント機器も、自己のデータ処理サービスを他のクライアントに提供する場合には、サーバとしての機能を提供可能となる。従って、図1に示すネットワーク接続されたクライアント機器もサーバとなり得る。

【0034】

ネットワーク100は、有線、無線等いずれかのネットワークであり、各接続機器は、MAC(Media Access Control)アドレスを有している。各ネットワーク接続機器は、宛先MACアドレスおよび送信元MACアドレスをヘッダ情報に持つパケット、例えばイーサネット(登録商標)フレームをネットワーク100を介して送受信する。すなわち、クライアントは、イーサネットフレームのデータ部に処理要求情報を格納したフレームをサーバ101に送信することにより、サーバ101に対するデータ処理要求を実行する。サーバ101は、処理要求フレームの受信に応じて、後述するアクセス権限判定処理を行ない、権限ありの判定を条件としてデータ処理を実行し、必要に応じてデータ処理結果としての結果データをイーサネットフレームのデータ部に格納し、各クライアントに送信する。

【0035】

ネットワーク接続機器は、例えばユニバーサルプラグアンドプレイ（U P n P : Universal Plug and Play）対応機器によって構成される。従って、ネットワークに対する接続機器の追加、削除が容易な構成である。ネットワークに新たに接続する機器は、

- (1) I P アドレス等の自己のデバイス I D を取得するアドレッシング処理。
- (2) ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。
- (3) ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスを受領することが可能となる。

【 0 0 3 6 】

図 1 に示すサーバおよびクライアント機器を構成する P C 等の情報処理装置のハードウェア構成例について図 2 を参照して説明する。

【 0 0 3 7 】

C P U (Central Processing Unit) 3 0 1 は、R O M (Read Only Memory) 3 0 2、または H D D 3 0 4 等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。R A M 3 0 3 には、C P U 3 0 1 が実行するプログラムやデータが適宜記憶される。C P U 3 0 1、R O M 3 0 2、および R A M 3 0 3、H D D 3 0 4 は、バス 3 0 5 を介して相互に接続されている。

【 0 0 3 8 】

バス 3 0 5 には、入出力インタフェース 3 0 6 が接続されており、この入出力インタフェース 3 0 6 には、例えば、ユーザにより操作されるキーボード、スイッチ、ボタン、あるいはマウス等により構成される入力部 3 0 7、ユーザに各種の情報を提示する L C D、C R T、スピーカ等により構成される出力部 3 0 8 が接続される。さらに、データ送受信手段として機能する通信部 3 0 9、さらに、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムー

バブル記録媒体 311 を装着可能で、これらのリムーバブル記録媒体 311 からのデータ読み出しあるいは書き込み処理を実行するドライブ 310 が接続される。

【0039】

図 2 に示す構成は、図 1 に示すネットワーク接続機器の一例としてのサーバ、パーソナルコンピュータ（PC）の例であるが、ネットワーク接続機器は PC に限らず、図 1 に示すように携帯電話、PDA 等の携帯通信端末、その他の様々な電子機器、情報処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。

【0040】

本発明において、アクセス制御を行なうネットワーク接続機器としての情報処理装置は、アクセス権限を有するネットワーク接続機器の機器リストとしてアクセス権限を有するネットワーク接続機器の MAC アドレスを登録した MAC アドレステーブルを格納し、MAC アドレステーブルに基づくアクセス制御処理を実行する。

【0041】

MAC アドレステーブルに基づくアクセス制御を実行する情報処理装置は、2 つのアクセス制御モードを持つ。すなわち、

- (1) 自動登録アクセス制御モード
- (2) 登録デバイスアクセス制御モード

の 2 つのモードである。

【0042】

(1) 自動登録アクセス制御モードは、MAC アドレステーブルに基づくアクセス制御を実行する情報処理装置が、外部機器（クライアント）からのアクセス要求を受信した場合に、アクセス要求パケットから送信元 MAC アドレス（クライアント MAC アドレス）を取得し、情報処理装置に格納した MAC アドレステーブルに登録された登録済み MAC アドレスと一致するか否かを判定し、一致する場合には、アクセスを許可する。一致しない場合には、アクセス要求パケット

から取得したMACアドレスをMACアドレステーブルに自動登録し、登録処理が実行されたことを条件としてアクセスを許容する。

【0043】

ただし、MACアドレステーブルに対するMACアドレス登録数には予め登録限度数：N（例えばN＝5，10，15，63など）が設定され、MACアドレステーブルの登録MACアドレス数が登録限度数：Nに達していない場合に限り、MACアドレスの自動登録処理が実行され、自動登録処理の後、アクセスが許可される。

【0044】

(2) 登録デバイスアクセス制御モードは、MACアドレステーブルに基づくアクセス制御を実行する情報処理装置が、外部機器（クライアント）からのアクセス要求を受信した場合に、アクセス要求パケットから送信元MACアドレス（クライアントMACアドレス）を取得し、情報処理装置に格納したMACアドレステーブルに登録された登録済みMACアドレス中、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理がなされたマニュアル登録MACアドレスと一致するか否かを判定し、マニュアル登録MACアドレスと一致する場合には、アクセスを許可する。一致しない場合には、アクセスを許可しない処理を実行するモードである。

【0045】

本発明の情報処理装置においては、上記2つのモードを適宜切り替えることを可能とし、各設定モードにおいて、上記態様でのアクセス制御を行う。

【0046】

本発明の情報処理装置がアクセス制御を行うために、記憶部に格納するMACアドレステーブル（MACリスト）の構成例について、図3を参照して説明する。アクセス制御を行なうネットワーク接続機器としての情報処理装置410は、ネットワークを介して接続される様々な情報処理装置421～423からアクセス要求を受領し、そのアクセス要求に含まれる送信元MACアドレスと、MACアドレステーブル（MACリスト）411に格納されたMACアドレスとの照合を行う。

【0047】

情報処理装置 410 が記憶部に格納している MAC アドレステーブル (MAC リスト) 411 は、図に示すように、登録限度数: N までのエントリを格納することを許容したテーブル構成を持ち、上述の自動登録アクセス制御モードまたは、予め定められたシーケンスに従ってマニュアル登録がなされた MAC アドレスデータが格納されている。

【0048】

さらに、MAC アドレステーブル (MAC リスト) 411 には、登録 MAC アドレスがマニュアル登録されたデータであるか否かのデータが各 MAC アドレスに対応付けられたデータとして設定される。

【0049】

すなわち、予め設定された登録シーケンスに従ったマニュアル登録処理によって登録された MAC アドレスであるか、あるいは上述の自動登録アクセス制御モードにおいて自動登録されたアドレスであるかを示すマニュアル登録識別データが、MAC アドレステーブル 411 に各登録 MAC アドレスに対応して設定される。図 3 において、マニュアル登録欄に○の設定されたエントリが予め設定された登録シーケンスに従ったマニュアル登録処理によって登録された MAC アドレスである。

【0050】

MAC アドレステーブルは、アクセス制御を行なうネットワーク接続機器としての情報処理装置 (サーバ) 内の記憶部 (不揮発性メモリ) に格納される。MAC アドレステーブルは、スロット単位で、各クライアントの登録データを格納する構成を有し、1 スロット毎に 1 つの登録クライアント情報を格納する。なお、登録情報には、図に示すようにクライアントの MAC アドレスと、マニュアル登録か否かの情報の他、図には示していないが、ユーザが任意に設定可能なクライアント名、登録日時等の情報を格納してもよい。

【0051】

[モードに応じたアクセス制御処理]

次に、アクセス制御を行なうネットワーク接続機器としての情報処理装置が実

行するアクセス制御処理シーケンスについて図4のフローを参照して説明する。

【0052】

ステップS101において、アクセス制御を行なうネットワーク接続機器としての情報処理装置は、他のネットワーク接続機器からのアクセス要求を受信する。アクセス制御を行なうネットワーク接続機器としての情報処理装置をサーバ、アクセス要求を実行する情報処理装置をクライアントとして説明する。

【0053】

クライアントから送信されるアクセス要求パケット（イーサネットフレーム）の構成例を図5に示す。パケットは、ヘッダ部、データ部、トレーラ部に区分され、ヘッダ部には、同期信号、パケット開始符号、宛先MACアドレス、送信元MACアドレス、およびパケット長、タイプが含まれる。

【0054】

データ部には、例えばTCP/IP通信プロトコルに従って生成されたデータが含まれ、例えば送信元、送信先IPアドレスを含むIPパケットが格納される。

【0055】

サーバは自己のアクセス制御モードが（1）自動登録アクセス制御モード、（2）登録デバイスアクセス制御モードのいずれにあるかによって異なる処理を実行することになる。サーバはステップS102において自己のモードを識別し、（1）自動登録アクセス制御モードにある場合は、ステップS103以下の処理を実行する。

【0056】

ステップS103では、クライアントからの受信パケットからアクセス要求元のMACアドレスを取得し、サーバの記憶部に格納したMACアドレステーブル（図3参照）に登録されたMACアドレスとの照合処理を実行し、登録済みか否かを判定する。登録済みである場合（ステップS103：Yes）は、ステップS106に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

【0057】

登録済みでない場合（ステップS103：No）は、ステップS104に進み、MACアドレステーブルにすでに登録されたMACアドレスがサーバに設定した登録限度数：Nに達していないか、すなわち、登録MACアドレス<登録限度数：Nであるか否かを判定する。

【0058】

登録MACアドレス<登録限度数：Nである場合（ステップS104：Yes）は、クライアントからの受信パケットのヘッダ部に設定されている送信元MACアドレスをMACアドレステーブルに登録し、その後、ステップS106においてアクセスを許可し、クライアントの要求に応じた処理を実行する。

【0059】

登録MACアドレス<登録限度数：Nでない場合（ステップS104：No）、すなわち、MACアドレステーブルに既に登録限度数：NのMACアドレスが登録済みである場合は、これ以上の自動登録を実行できないので、MACアドレスの登録処理を実行することなく、ステップS107において、クライアントからのアクセス要求を拒絶する。

【0060】

一方、ステップS102において、自己のモードが、（2）登録デバイスアクセス制御モードであると判定した場合は、ステップS111に進み、クライアントからの受信パケットからアクセス要求元のMACアドレスを取得し、サーバの記憶部に格納したMACアドレステーブル（図3参照）に登録されたMACアドレス中、予め規定されたMACアドレス登録処理シーケンスに従ったマニュアル登録処理がなされたマニュアル登録MACアドレスと一致するか否かを判定する。

【0061】

すなわち、図3において、マニュアル登録欄に○の設定されたエントリのみが照合処理対象のMACアドレスエントリとなる。送信元MACアドレス（クライアントMACアドレス）が、マニュアル登録されたMACアドレスエントリと一致する場合（ステップS111：Yes）には、ステップS106に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

【 0 0 6 2 】

一方、送信元MACアドレスが、マニュアル登録されたMACアドレスエントリと一致しない場合（ステップS 1 1 1 : N o）には、ステップS 1 1 2に進み、アクセスを拒絶する。

【 0 0 6 3 】

登録デバイスアクセス制御モードにある場合は、送信元MACアドレスが、MACアドレステーブルに自動登録されたMACアドレスと一致する場合であってもアクセスを拒絶することになる。

【 0 0 6 4 】

なお、アクセス制御を行なうネットワーク接続機器としての情報処理装置（サーバ）が（1）自動登録アクセス制御モードにある場合、サーバは、クライアントからの要求態様を判定し、特定のカテゴリのアクセス要求である場合にのみ、アクセス制御を実行、すなわち、MACアドレステーブルとの照合および自動登録処理を実行し、特定のカテゴリのアクセス要求でない場合には、アクセス制御を実行することなく、すなわち、MACアドレステーブルとの照合および自動登録処理を実行することなくクライアントからの要求に応じる構成としてもよい。

【 0 0 6 5 】

特定のカテゴリのアクセス要求とは、例えば、サーバの保有するコンテンツの取得要求や、サーバに対する制御要求である。例えばUPnP機器において、サーバの保有するコンテンツの取得要求は、コンテンツの識別子としてのコンテンツURL（Uniform Resource Locators）を指定したHTTP（Hyper Text Transfer Protocol）GETメソッドに基づいて実行される。また、サーバに対する制御要求はSOAP（Simple Object Access Protocol）プロトコルが利用される。

【 0 0 6 6 】

アクセス制御を行なうネットワーク接続機器としての情報処理装置（サーバ）が（1）自動登録アクセス制御モードにある場合、クライアントからの要求が、コンテンツURL（Uniform Resource Locators）を指定したHTTP（Hyper Text Transfer Protocol）GETメソッドであるか、あるいは、SOAP（Simple

Object Access Protocol) プロトコルに基づくサーバに対する制御要求である場合にのみ、アクセス制御処理としてのMACアドレステーブルとの照合および自動登録処理を実行し、MACアドレステーブルに登録済みであることを条件としてアクセス要求を許容する。クライアントからのアクセスがHTTP-GETメソッドに基づくコンテンツ取得要求、あるいはSOAPに基づく制御要求以外、例えば、UPnPにおける機器発見処理としてのディスカバリ要求である場合などには、アクセス制御処理としてのMACアドレステーブルとの照合および自動登録処理を実行することなく、無条件にクライアントの要求を受領し、応答を実行する。

【0067】

サーバにおいて、クライアントからの要求種別を判別して、アクセス制御処理としてのMACアドレステーブルとの照合および自動登録処理を実行するか否かを判定して処理を実行するシーケンスについて、図6のフローチャートを参照して説明する。

【0068】

図6の処理フローは、アクセス制御を行なうネットワーク接続機器としての情報処理装置（サーバ）が自動登録アクセス制御モードにある場合の処理である。

【0069】

ステップS201において、アクセス制御を行なうネットワーク接続機器としての情報処理装置は、他のネットワーク接続機器からのアクセス要求を受信する。ステップS202では、クライアントからのアクセス要求が、HTTP-GETメソッドに基づくコンテンツ取得要求、あるいはSOAPに基づく制御要求であるか否かを判定する。

【0070】

クライアントからのアクセス要求が、HTTP-GETメソッドに基づくコンテンツ取得要求、あるいはSOAPに基づく制御要求である場合（ステップS202: Yes）には、ステップS203において、受信パケットからアクセス要求元のMACアドレスを取得し、サーバの記憶部に格納したMACアドレステーブル（図3参照）に登録されたMACアドレスとの照合処理を実行し、登録済み

可否かを判定する。登録済みである場合（ステップS203：Yes）は、ステップS206に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

【0071】

登録済みでない場合（ステップS203：No）は、ステップS204に進み、MACアドレステーブルにすでに登録されたMACアドレスがサーバに設定した登録限度数：Nに達していないか、すなわち、登録MACアドレス<登録限度数：Nであるかを判定する。

【0072】

登録MACアドレス<登録限度数：Nである場合（ステップS204：Yes）は、ステップS205において、クライアントからの受信パケットのヘッダ部に設定されている送信元MACアドレスをMACアドレステーブルに登録し、その後、ステップS206においてアクセスを許可し、クライアントの要求に応じた処理を実行する。

【0073】

登録MACアドレス<登録限度数：Nでない場合（ステップS204：No）は、すなわち、MACアドレステーブルに既に登録限度数：NのMACアドレスが登録済みである場合は、これ以上の自動登録を実行できないので、MACアドレスの登録処理を実行することなく、ステップS207において、クライアントからのアクセス要求を拒絶する。

【0074】

一方、ステップS202において、クライアントからのアクセス要求が、HTTP-GETメソッドに基づくコンテンツ取得要求、あるいはSOAPに基づく制御要求でないと判定した場合には、MACアドレステーブルとの照合、自動登録処理を実行することなく、ステップS206に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

【0075】

図7に、アクセス制御を実行するネットワーク接続機器（サーバ）のアクセス制御処理を説明する機能ブロック図を示す。サーバは、ネットワークを介したパ

ケットの送受信を実行するパケット送受信部501、パケット送受信部501を介して受信するパケットの解析および、パケット送受信部501を介して送信するパケットを生成するパケット生成、解析部502、クライアントから受信するパケットに基づいてMACアドレステーブルに対する登録可否を判定し、登録可と判定した場合にMACアドレスの登録処理を実行する登録処理実行部503、MACアドレステーブルを格納した記憶部504、さらに、サーバに対する様々なデータ処理要求パケットに基づいて、データ処理要求クライアントがMACアドレステーブルに登録されているか否か等を判断し、アクセス可否判定処理を実行するアクセス制御処理実行部505、アクセス制御処理実行部505におけるアクセス可の判定を条件として、クライアントの要求するデータ処理を実行するデータ処理部507、サーバが(1)自動登録アクセス制御モードにあるか、(2)登録デバイスアクセス制御モードにあるかのモード情報を記憶したモード情報記憶部506を有する。

【0076】

登録処理実行部503、アクセス制御処理実行部505は、モード情報記憶部506に設定されたモード設定情報、すなわち、(1)自動登録アクセス制御モード、(2)登録デバイスアクセス制御モードの2つのモードのいずれのモードにあるかに応じて異なる処理を実行する。例えば、(1)自動登録アクセス制御モードにある場合は、登録処理実行部503は、記憶部504に記憶されたMACアドレステーブルの登録エントリ数に基づいて、自動登録が許容されるか否かの判定を実行し、限度数以内であることを条件とした登録処理を実行する。

【0077】

また、登録処理実行部503は、マニュアル登録処理実行時における登録可否判定処理も実行する。すなわち予め決められたマニュアル登録処理シーケンスに応じた処理が実行されているか否かを判定する処理などを実行する。なお、マニュアル登録処理の詳細例については後述する。

【0078】

図8にアクセス制御を実行するネットワーク接続機器(サーバ)においてディスプレイに表示されるMACアドレステーブルおよびモード設定処理を実行する

ためのユーザインタフェースの例を示す。

【0079】

サーバのディスプレイ650には、クライアント機器名、MACアドレス、マニュアル登録か否かを示すデータからなるMACアドレステーブル651が表示され、さらに、現在の設定モード情報表示部652、モード切り替え部654とマニュアル登録処理においてMACアドレスを登録する際の登録確認ボタン655を持つユーザ入力部653、さらにMACアドレステーブル651に登録されたエントリを削除するための削除ボタン656を持つユーザインタフェース（UI）が表示される。

【0080】

クライアントからのアクセス要求である、すべてのHTTP-GETメソッドおよびSOAPには、図9のような送信者の情報を示すHTTP拡張ヘッダ（X-AV-Client-Info）が付加されており、ディスプレイ650には、この情報に基づく表示処理がなされる。すなわち、例えば、図9に示すように、

```
GET /tracks/track?id=254 HTTP/1.1 ¥r¥n
```

```
Host:192.254.32.11:80 ¥r¥n
```

```
X-AV-Client-Info: av=2.0 ; cn =Sony Corporation ;mn=Linux-Sample-CP ; mv  
=2002-11-22-2.0 ¥r¥n
```

からなるHTTP拡張ヘッダ（X-AV-Client-Info）がクライアントから送信される。

【0081】

ユーザは、図8に示すようなUIをサーバのディスプレイに表示し、モードの切り替えを実行し、また、MACアドレステーブルに登録されたMACアドレスの確認を実行することができ、さらに、必要に応じてMACアドレステーブルに登録されたMACアドレスの削除処理を実行する。

【0082】

[マニュアル登録処理]

次に、アクセス制御を実行する情報処理装置が実行するMACアドレスのマニ

ュアル登録処理の手順について、図10のシーケンス図を参照して説明する。なお、図10に示す例は、マニュアルによるMACアドレス登録処理の一例であり、必ずしもこの例に従ったマニュアル登録を行うことが必須ではない。ただし、あらかじめ定められたマニュアル登録を行ったクライアントのMACアドレスのみが、図3に示すMACアドレステーブル（MACリスト）にマニュアル登録されたMACアドレスとしてエントリが設定される。

【0083】

図10に示すシーケンスは、パスワードを用いた機器認証に基づくMAC登録処理シーケンスである。まず、ステップS301において、ユーザがクライアント（コントローラ）側に設けられた登録ボタンを押下する。すると、クライアント装置は登録ボタンの押下に応じて発生するユーザシグナルA（USA）に従い、ステップS302において、MACアドレス登録要求をネットワークを介してブロードキャスト送信する。MACアドレス登録要求のブロードキャスト送信は、例えば3秒毎に数分間継続して実行される。

【0084】

クライアント（コントローラ）側に設けられた登録ボタンを押下した後、ユーザはサーバ（デバイス）側に移動する。そして、ステップS303において、サーバ側に設けられた確認ボタンを押下する。すると、サーバは確認ボタンの押下に応じて発生するユーザシグナルB（USB）に従い、ステップS304において、MACアドレス登録要求を規定時間、例えば10秒間受信する。

【0085】

10秒間に同一の送信元（MACアドレス）からMACアドレス登録要求を受信した場合、サーバはそのMACアドレスをMACアドレステーブル（MACリスト）（図3参照）に仮記憶した後、ユーザに対して「機器を発見しました。登録しますか？」なるメッセージを表示するデバイスシグナルA（DSA）を発生（S305）し、その状態で所定時間（たとえば1分間）待機する。

【0086】

なお、サーバは、MACアドレステーブルを参照し、既にマニュアル登録済みのクライアントからのMACアドレス登録要求であると判定した場合、MAC登

録完了を意味する通知をクライアントに送信してMACアドレス登録処理を終了する。すなわちサーバは同一のMACアドレスの二重登録は行わない。

【0087】

ただし、マニュアル登録されていないが、自動登録処理によってMACアドレステーブルに登録されているMACアドレスと一致するMACアドレスのマニュアル登録処理である場合は、サーバは、MACアドレステーブルに登録されているMACアドレスデータエントリを自動登録エントリからマニュアル登録エントリへ変更する処理を行う。

【0088】

この変更処理においては、サーバは、MACアドレステーブルの自動登録処理のなされたMACアドレスデータのエントリに対応するマニュアル登録フィールドにマニュアル登録がなされたことを示す識別子を設定する処理を実行することになる。

【0089】

サーバが、ステップS305において、「機器を発見しました。登録しますか？」なるメッセージを表示するデバイスシグナルA(DSA)を発生した状態で所定時間(例えば1分間)待機している間に、ステップS306において、ユーザがサーバ側に設けられた確認ボタン(図8の登録確認ボタン655)を押下する。すると、サーバは確認ボタンの押下に応じて発生するユーザシグナルC(USC)に従い、ステップS307において、MAC登録確認要求をクライアントに対して送信する。MAC登録確認要求には、パスワード要求フラグが付加される。

【0090】

クライアントは、パスワード要求フラグが付加されたMAC登録確認要求をサーバから受信すると、ステップS308において、受信したMAC登録確認要求に含まれるパスワード要求フラグに基づき、ユーザに対して「デバイス“XXX X”のパスワードを入力してください。」なるメッセージを表示するデバイスシグナルB(DSB)を発生し、パスワードの入力を所定時間(例えば5分間)待機する。

【0091】

さらに、クライアントは、MACアドレス登録要求の送信を停止し、ステップ S309において、サーバへMAC登録確認レスポンスを返信する。

【0092】

サーバは、このMAC登録確認レスポンスを受信すると、ステップS310において、パスワード（ワンタイムパスワード）を生成し、ユーザに対して「クライアント（コントローラ）“YYYY”のためのパスワードは”〇〇〇〇”です。」なるメッセージを表示するデバイスシグナルC（DSC）を発生し、パスワードを提示した状態で規定時間（例えば5分間）待機する。

【0093】

一方、クライアント側では、パスワードの入力待機中に、ステップS311で、ユーザがパスワードを入力すると、ステップS312で、クライアントから入力パスワードがサーバに送信される。

【0094】

サーバは、パスワードをクライアントから受信すると、ステップS310で生成しサーバ側でユーザに対して提示したパスワードと、受信パスワードとの照合処理を実行する。クライアントからの受信パスワードと生成パスワードとが一致すると、ステップS313において、サーバはMACアドレステーブル（MACリスト）（図3参照）にクライアントのMACアドレスを正式エン트리として設定するとともに、マニュアル登録であることを示す識別データ（フラグなど）を設定する。または自動登録エントリをマニュアル登録エントリに変更する。

【0095】

サーバはMACアドレスの登録が済むと、ステップS314において、ユーザに対して「クライアント（コントローラ）“YYYY”を登録しました。」なるメッセージを表示するデバイスシグナルD（DSD）を発生し、ステップS315において、クライアントに照合OKを付加したパスワードレスポンスを返信する。

【0096】

クライアントは、サーバからパスワード照合OKに基づくMACアドレス登録

通知としてのパスワードレスポンスを受信すると、ステップ S 3 1 6 において、MAC アドレスが認証登録されたとして、ユーザに対して「デバイス “X X X X” に登録されました。」なるメッセージを表示するデバイスシグナル E (D S E) を発生して MAC アドレスの機器認証を伴うマニュアル登録処理を終える。

【0097】

なお、クライアントから送られてきたパスワードが不正、すなわちクライアントからの受信パスワードとサーバの生成パスワードが不一致であると、サーバはクライアントに照合 NG を付加したパスワードレスポンスを返信し、クライアントから再度パスワード入力されるのを待機し、待機期間中にパスワード照合 NG が 3 回連続すると、サーバはパスワード入力の再試行を中止させ、ユーザに対して「コントローラ “Y Y Y Y” を登録できません。」なるメッセージを表示し、クライアントの MAC アドレス登録を実行することなく処理を終了する。

【0098】

上述した MAC アドレスのマニュアル登録処理を実行したクライアントの MAC アドレスのみが、MAC アドレステーブルにマニュアル登録 MAC アドレスとして登録されることになる。

【0099】

サーバが「登録デバイスアクセス制御モード」にある場合は、これらのマニュアル登録されたクライアントのみが、アクセスを許容されることになる。

【0100】

〔サーバおよびクライアントの機能構成〕

サーバおよびクライアント装置のハードウェア構成については、先に図 2 を参照して説明した通りであり、上述した各種の処理は、サーバクライアントそれぞれの記憶部に格納されたプログラムに従って制御部としての CPU が実行する。

【0101】

CPU によって実行される処理は、例えばサーバ側では、クライアントからの要求を入力し、入力情報の解析、解析結果に基づく MAC アドレステーブル (MAC リスト)、すなわちアクセス制御情報へ登録する処理、クライアントと送受信するパケット生成、解析処理、さらに、登録処理における各種メッセージ出力

、ユーザ入力情報の解析処理等である。クライアント側の処理としては、サーバに対する各種要求パケットの生成、送信、サーバから受信するパケット解析処理、さらに、登録処理における各種メッセージ出力、ユーザ入力情報の解析処理等である

【0102】

基本的にこれらの処理は、サーバ、クライアント装置の制御部としてのCPUの制御の下に予め格納された処理プログラムに従って実行される。制御部としてのCPUが実行する処理および記憶部の格納データ等について、図11および図12を参照して説明する。図11は、サーバの主要機能構成を説明するブロック図であり、図12は、クライアントの主要機能構成を説明するブロック図である。

【0103】

まず、図11のサーバの機能構成を示すブロック図を参照してサーバの機能構成について説明する。パケット送受信部701は、クライアントに対するパケット、クライアントからのパケットを受信する。パケット生成、解析部702は、送信パケットの生成処理、受信パケットの解析処理を行う。パケットのアドレス設定、アドレス認識、パケットのデータ格納部に対するデータ格納、データ格納部からのデータ取得処理などである。

【0104】

データ入力部703は、ユーザによるデータ入力を実行するためのキーボード、ユーザインタフェースなどである。データ出力部704は、メッセージデータ等を表示するディスプレイ等の出力部である。

【0105】

アクセス制御処理実行部705は、先に図4、図6を参照して説明した(1)自動登録アクセス制御モードにおけるアクセス制御処理、(2)登録デバイスアクセス制御モードにおけるアクセス制御処理を実行する。

【0106】

登録処理部706は、(1)自動登録アクセス制御モードにおけるアクセスに対応して実行するMACアドレス登録処理と、先に図10を参照して説明したマ

ニユアル登録処理を実行する。すなわち、登録処理部 706 は、例えば、図 10 を参照して説明したマニュアル登録処理のように、予め規定された MAC アドレス登録処理シーケンスに従った処理が実行されたことを条件として、クライアント MAC アドレスを MAC アドレステーブルにマニュアル登録 MAC アドレスとして登録する処理を実行する。

【0107】

さらに、登録処理部 706 は、予め規定された MAC アドレス登録処理シーケンスに従ったマニュアル登録処理が実行された MAC アドレスが、自動登録 MAC アドレスとしてテーブルに登録されている場合は、自動登録クライアント MAC アドレスエントリをマニュアル登録クライアント MAC アドレスエントリとする設定変更処理を実行する。

【0108】

データ処理部 707 は、アクセスの許可されたクライアントからの要求、例えばコンテンツ取得処理等に対応する処理を実行する。記憶部 708 には、アクセス制御処理実行部 705 において実行するアクセス制御処理プログラム 711、登録処理部 706 において実行する MAC アドレス登録処理プログラム 712 等の各種データ処理プログラムが格納され、さらに、図 3 を参照して説明した MAC アドレステーブル 713、さらにサーバに設定されたモード情報 714 が格納される。なお、サーバはさらにクライアントに提供するコンテンツ、コンテンツに対応するメタデータ等を格納している。

【0109】

次に、クライアント装置の機能構成について、図 12 を参照して説明する。パケット送受信部 801 は、サーバに対するパケット、サーバからのパケットを受信する。パケット生成、解析部 802 は、送信パケットの生成処理、受信パケットの解析処理を行う。パケットのアドレス設定、アドレス認識、パケットのデータ格納部に対するデータ格納、データ格納部からのデータ取得処理などである。

【0110】

データ入力部 803 は、ユーザによるデータ入力を実行するためのキーボード、ユーザインタフェースなどである。データ出力部 804 は、メッセージデータ

等を表示するディスプレイ等の出力部である。

【0111】

アクセス要求処理実行部805は、コンテンツ取得要求、制御要求等のサーバに対する各種のアクセス要求処理を実行する。アドレス登録処理実行部806は、図10を参照して説明したMACアドレスのマニュアル登録処理を実行する。

【0112】

データ処理部は、サーバから取得したコンテンツの再生処理など、様々なデータ処理を実行する。記憶部808には、アドレス登録処理実行部806において実行するアドレス登録処理プログラム811他の処理プログラム、さらにクライアントのMACアドレス812などが格納される。

【0113】

サーバ、およびクライアントは、機能的には図11、図12に示す各機能を有し、上述した各処理を実行する。ただし、図11、図12に示すブロック図は、機能を説明するブロック図であり、サーバクライアントが図11、図12に示すブロックに対応するハードウェアを有することは必須ではない。具体的には、図2に示すPC等の構成におけるCPUの制御の下に各種の処理プログラムが実行され、図11、図12に示す各ブロックを参照して説明した処理、あるいは上述の発明の詳細な説明において説明した各処理が実行される。

【0114】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0115】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行

させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【0116】

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical)ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0117】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【0118】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0119】

【発明の効果】

以上、説明したように、本発明の構成においては、マニュアル登録のなされたクライアントMACアドレスと、自動登録処理のなされたクライアントMACアドレスとを識別可能な態様で登録したMACアドレステーブルを設定し、アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに

至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのMACアドレスが、MACアドレステーブルに、マニュアル登録されたMACアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成としたので、ユーザによるマニュアル登録処理を実行しない場合においても、無制限なアクセスが防止され、例えば不特定多数クライアントからのサーバ格納コンテンツの取得等を防止することが可能となり、さらに、モードを、登録デバイスアクセス制御モードに設定することにより、厳格なアクセス制御を実行することも可能となる。

【0120】

さらに、本発明の構成によれば、自動登録アクセス制御モードにおいて、クライアントのアクセス要求種別を識別し、識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別、例えばHTTP (Hyper Text Transfer Protocol) - GETメソッドに基づくコンテンツ要求処理、またはSOAP (Simple Object Access Protocol) に基づく制御要求処理である場合にのみ、クライアントのMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、該登録処理を条件としたアクセス許容を実行する構成としたので、UPnP等における機器発見処理、情報取得処理等において不必要なアクセス制御を行うことが防止される。

【図面の簡単な説明】

【図1】

本発明の適用可能なネットワーク構成例を示す図である。

【図2】

ネットワーク接続機器の構成例について説明する図である。

【図3】

本発明の情報処理装置の有するMACアドレステーブルおよびアクセス制御処理について説明する図である。

【図4】

本発明の情報処理装置の実行するアクセス制御処理について説明するフロー図である。

【図 5】

クライアントがソウシンするパケット構成を示す図である。

【図 6】

本発明の情報処理装置の実行するアクセス制御処理について説明するフロー図である。

【図 7】

本発明の情報処理装置のアクセス制御処理構成を示す機能ブロック図である。

【図 8】

アクセス制御処理を実行する情報処理装置のディスプレイに表示されるユーザインタフェース構成例を示す図である。

【図 9】

クライアントからのアクセス要求に含まれる HTTP-GET ヘッダのデータ例を示す図である。

【図 10】

MAC アドレスのマニュアル登録処理シーケンスの例を示すシーケンス図である。

【図 11】

サーバの機能構成を示すブロック図である。

【図 12】

クライアントの機能構成を示すブロック図である。

【符号の説明】

【符号の説明】

100 ネットワーク

101 サーバ

121, 122, 124 パーソナルコンピュータ (PC)

123 携帯電話

125 PDA

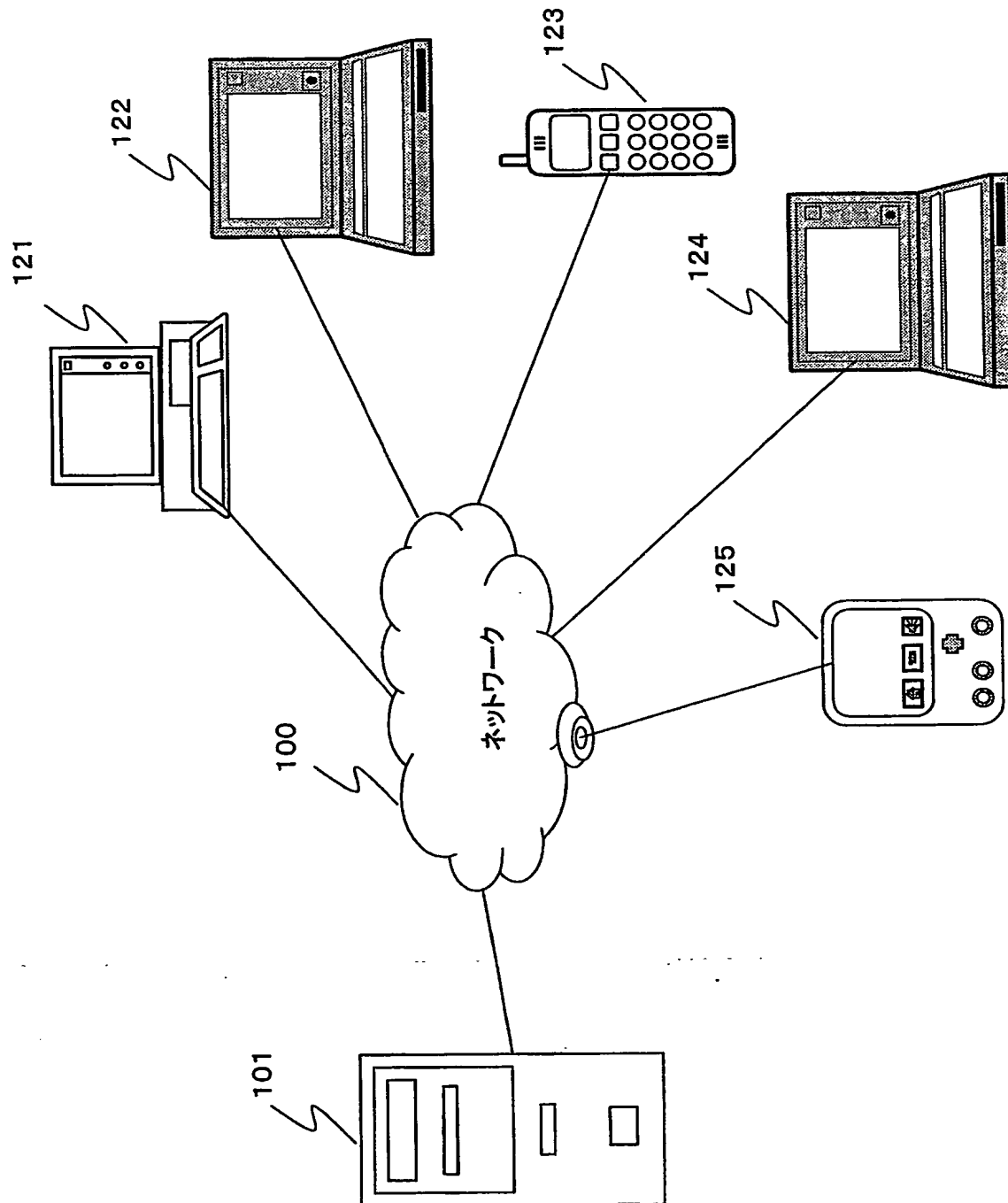
301 CPU
302 ROM
303 RAM
304 HDD
305 バス
306 入出力インタフェース
307 入力部
308 出力部
309 通信部
310 ドライブ
311 リムーバブル記録媒体
410 情報処理装置
411 MACアドレステーブル
421～423 情報処理装置
500 データ送受信部
501 パケット送受信部
502 パケット生成解析部
503 登録処理実行部
504 記憶部
505 アクセス制御処理実行部
506 モード情報記憶部
507 データ処理部
650 ディスプレイ
651 MACアドレステーブル
652 モード設定部
653 ユーザ入力部
654 モード切り替え部
655 登録確認ボタン
656 削除ボタン

- 701 パケット送受信部
- 702 パケット生成、解析部
- 703 データ入力部
- 704 データ出力部
- 705 アクセス制御処理実行部
- 706 登録処理実行部
- 707 データ処理部
- 708 記憶部
- 711 アクセス制御処理プログラム
- 712 マニュアル登録処理プログラム
- 713 MACアドレステーブル
- 714 モード設定情報
- 801 パケット送受信部
- 802 パケット生成、解析部
- 803 データ入力部
- 804 データ出力部
- 805 アクセス要求処理実行部
- 806 アドレス登録処理実行部
- 807 データ処理部
- 808 記憶部
- 811 アドレス登録処理プログラム
- 812 クライアントMACアドレス

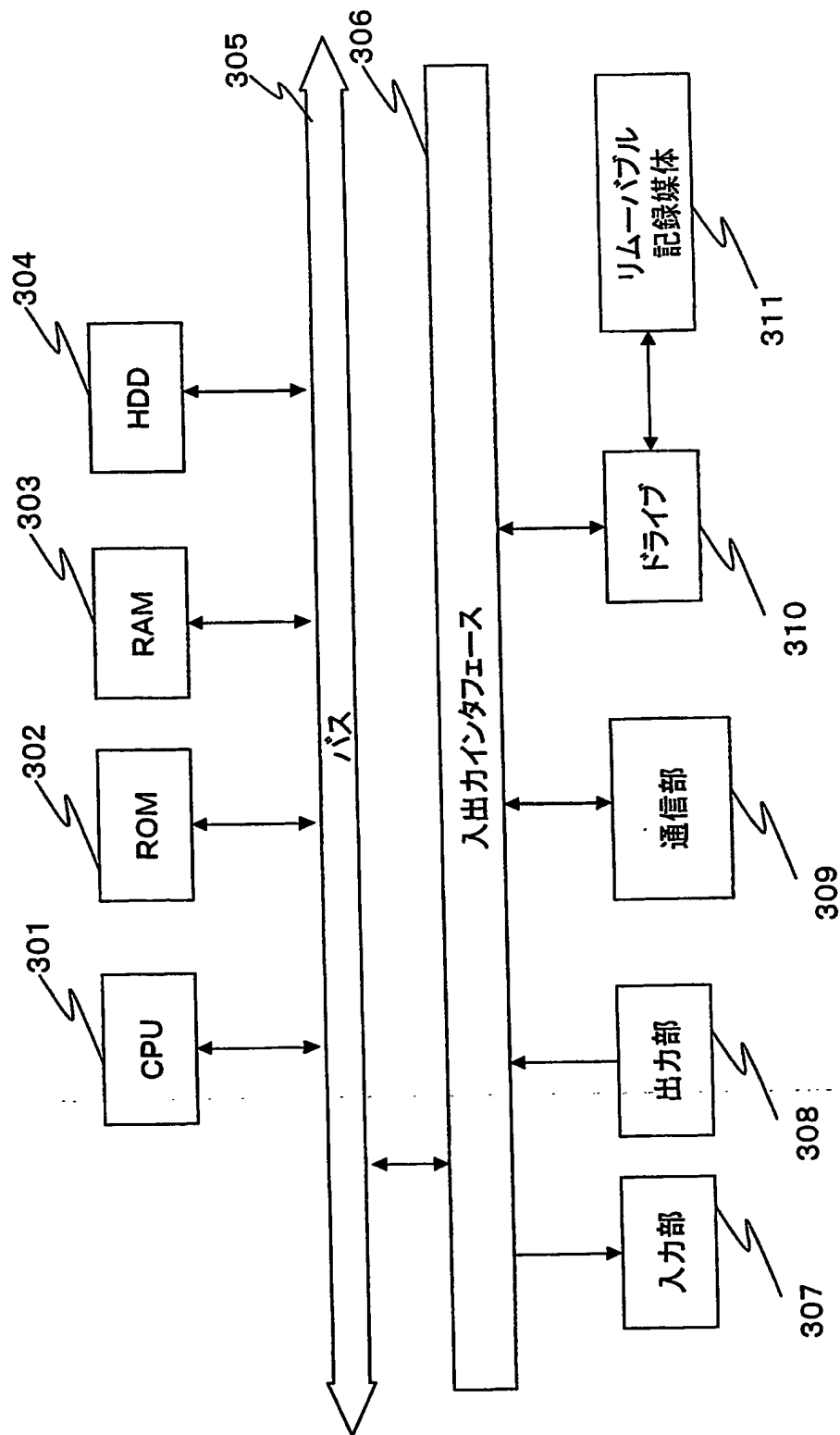
【書類名】

図面

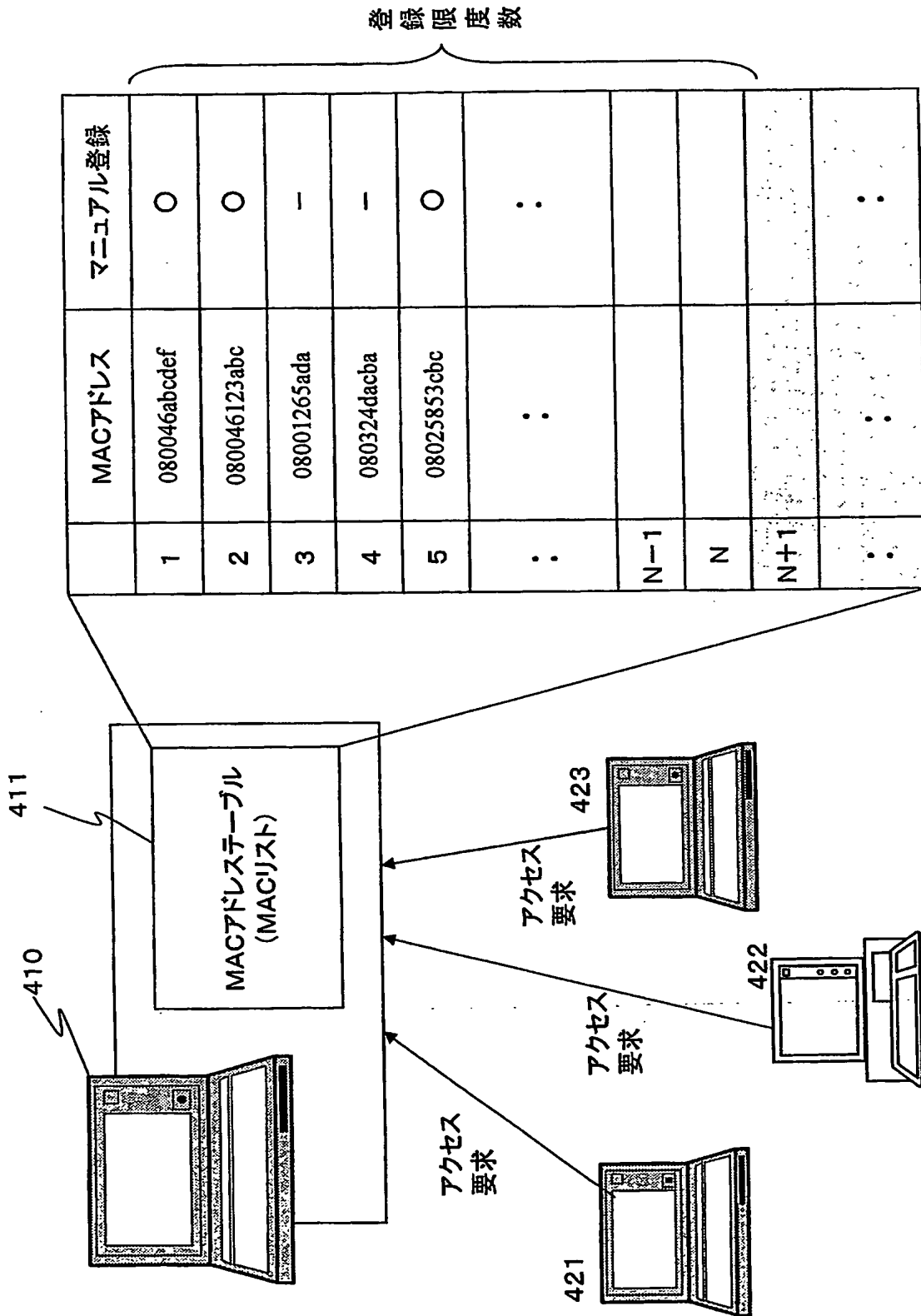
【図 1】



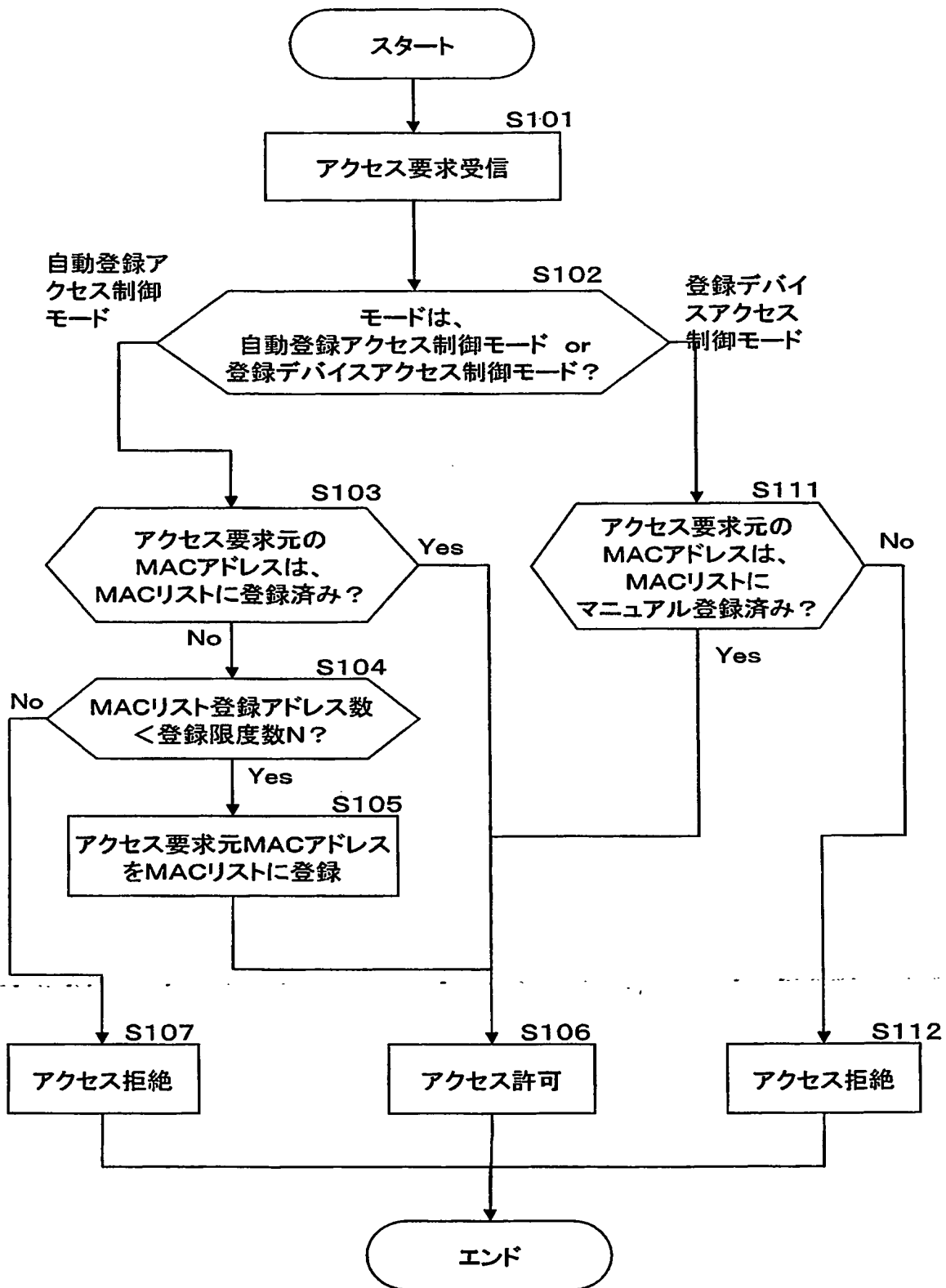
【図 2】



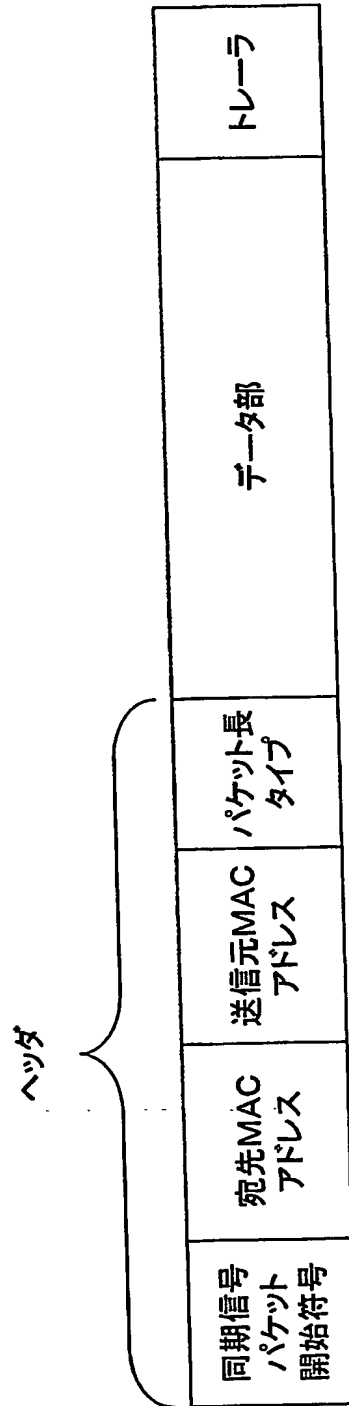
【図 3】



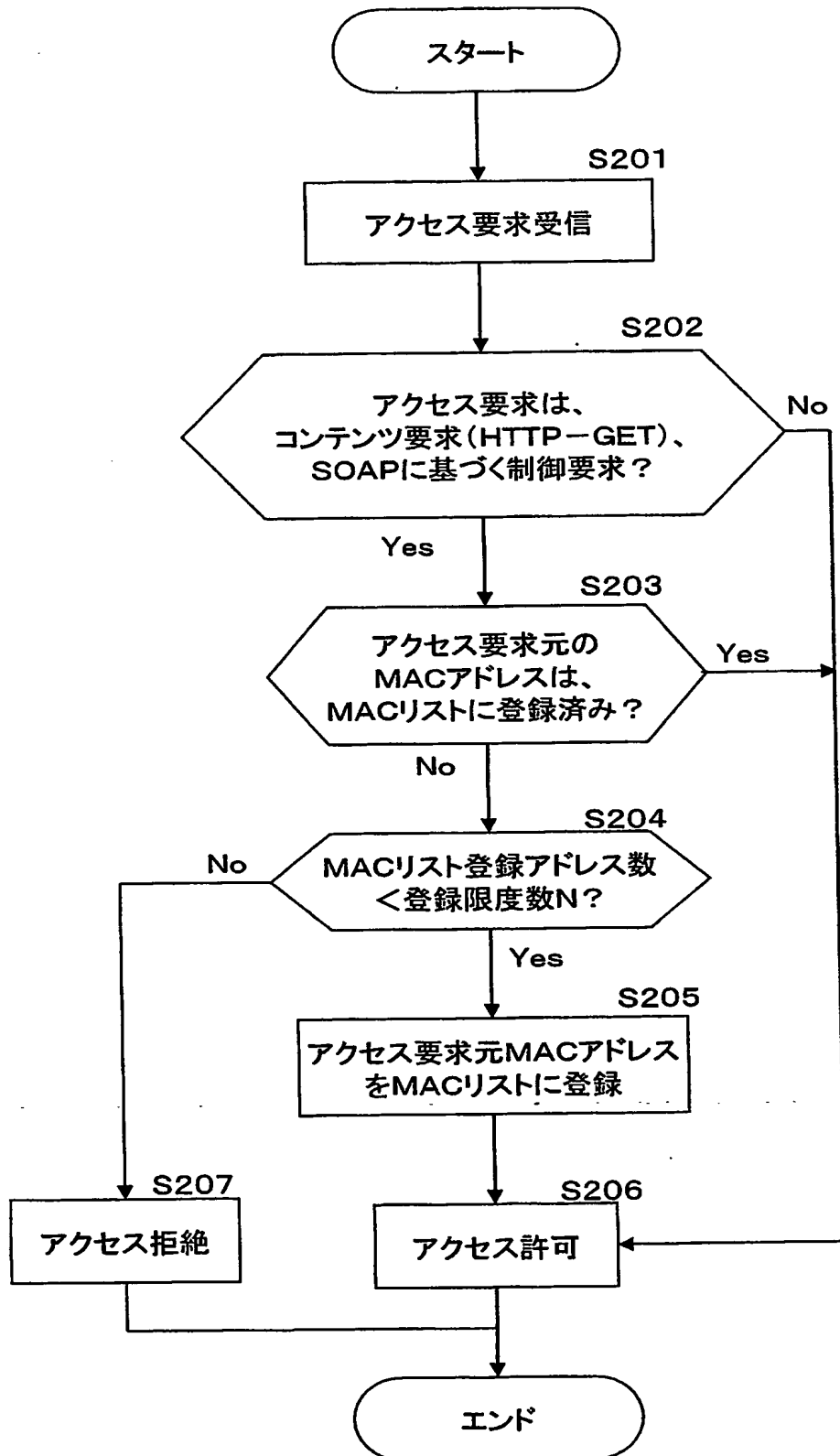
【図 4】



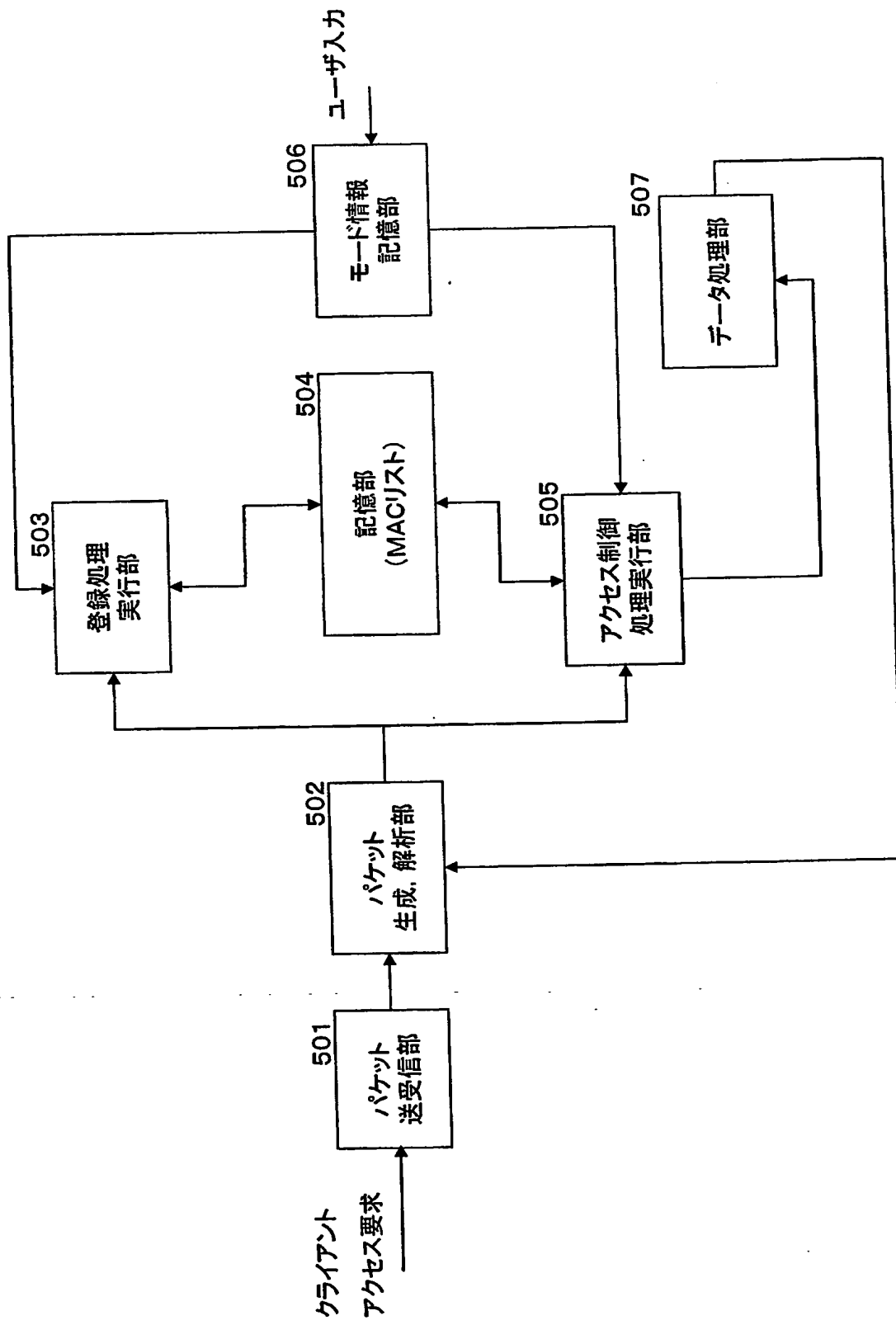
【図 5】



【図 6】



【図 7】



【図 8】

650

651

クライアント機器名.	MACアドレス	マニュアル登録
Bedroom PC	080046abcdef	○
MediaReceiver	080046123abc	○
TV	08001265ada	-
No Name	080324dacba	-

652

現在***
モードです。

653

登録削除

654

655

###モードにする。

クライアントを登録する。

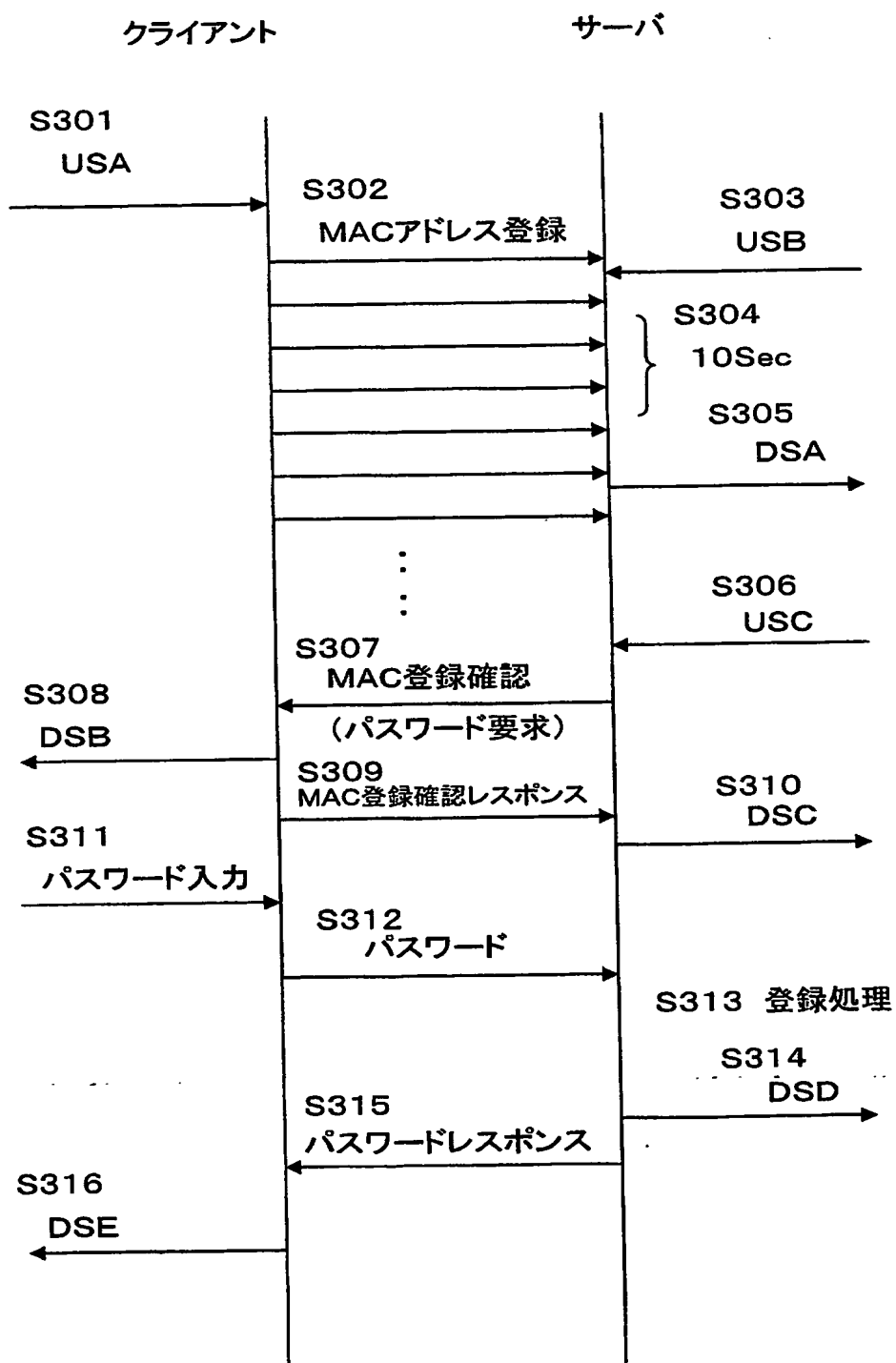
OK

キャンセル

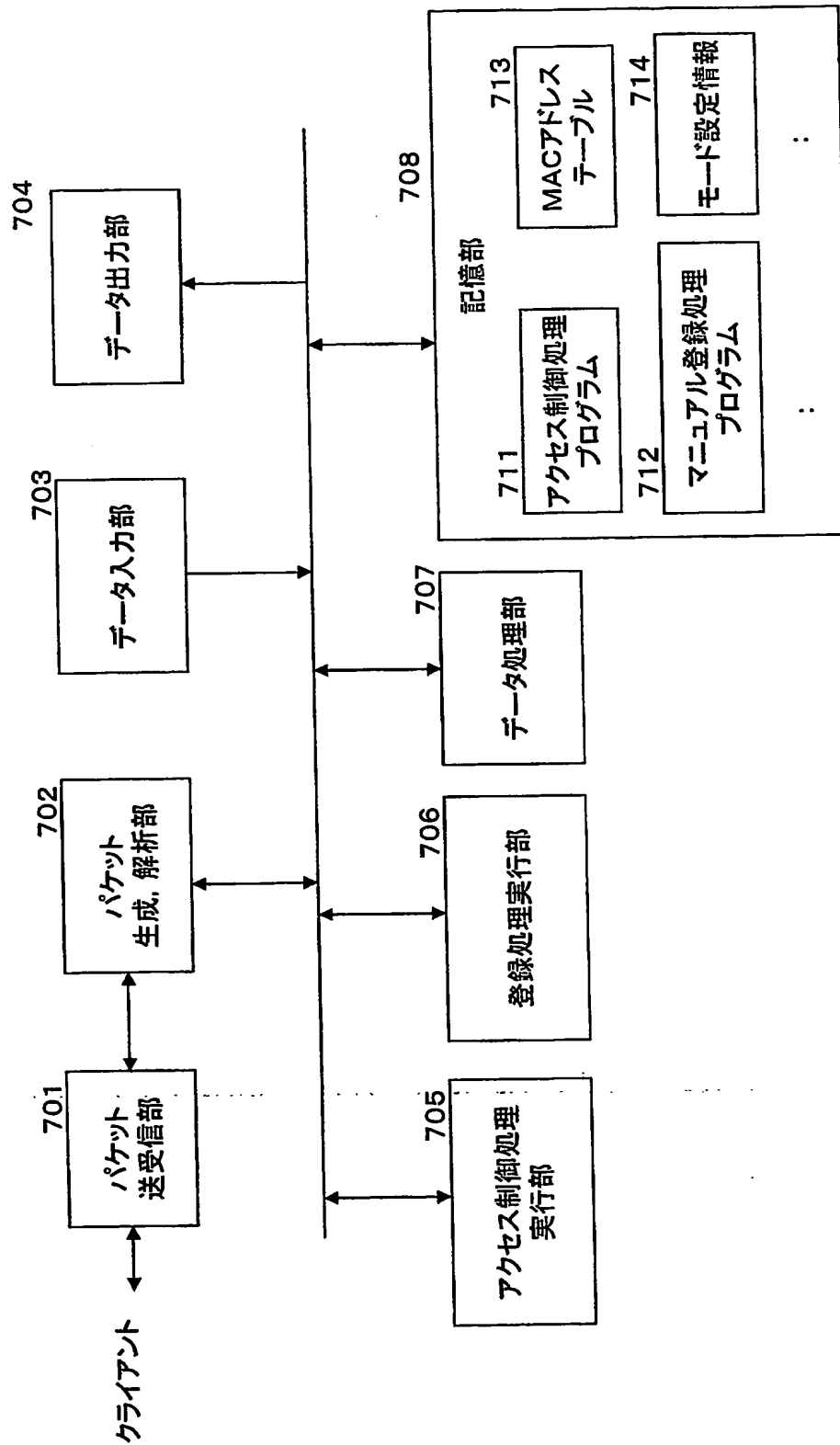
【図 9】

```
GET /tracks/track?id=254 HTTP/1.1 %n
Host: 192.254.32.11:80 %n
X-AV-Client-Info: av=2.0 ; cn = "Sony Corporation" ; mn=Linux-Sample-CP ; mv=2002-11-22-2.0 %n
```

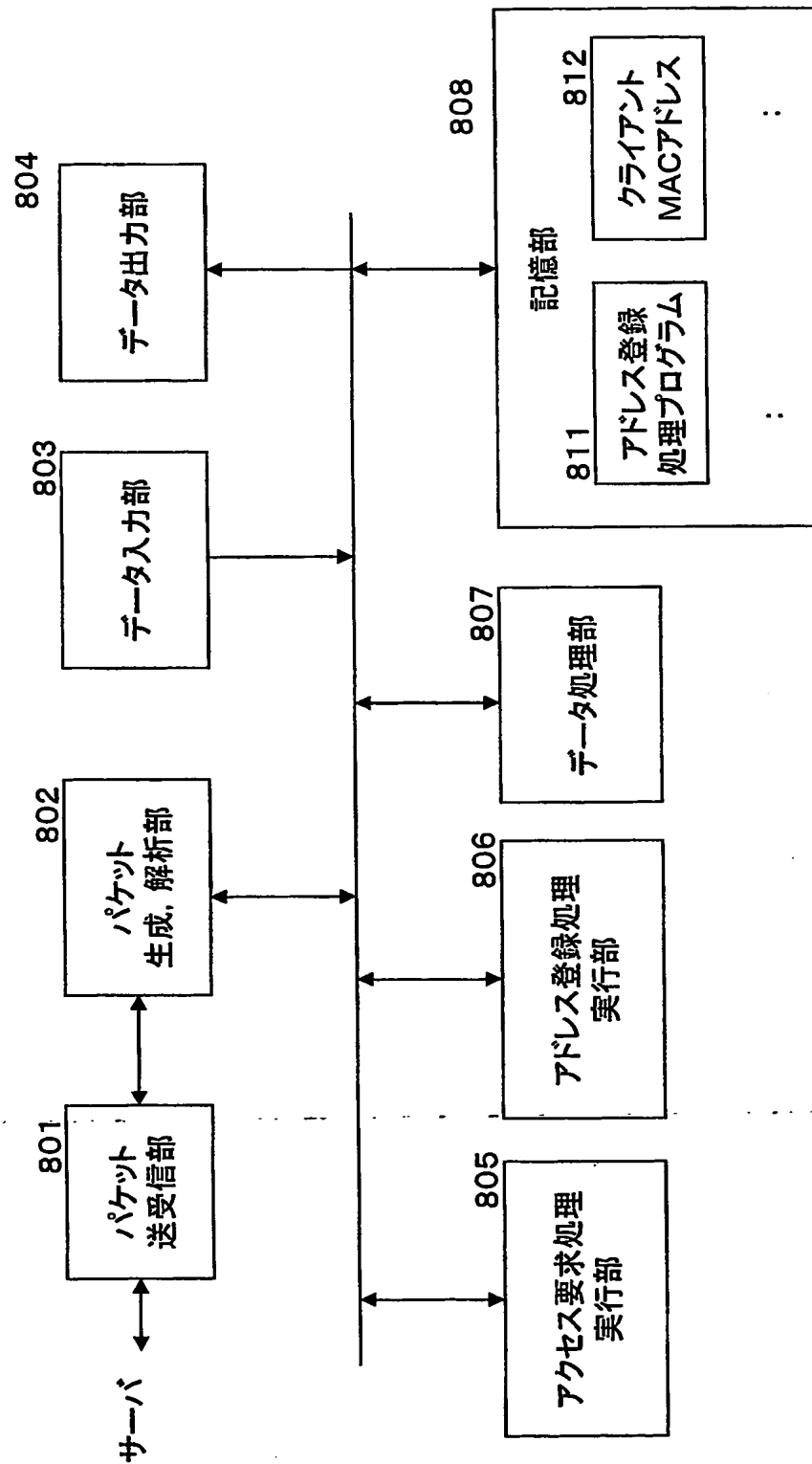
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【課題】 モード設定による異なるアクセス制御を可能とした装置および方法を実現する。

【解決手段】 マニュアル登録MACアドレスと、自動登録MACアドレスとを識別可能な態様で登録したMACアドレステーブルを設定し、アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントMACアドレスを、MACアドレステーブルの規定登録限度数：Nに至るまで登録し、登録を条件としてアクセスを許容し、アクセス制御モードが、登録デバイスアクセス制御モードである場合は、クライアントMACアドレスが、MACアドレステーブルに、マニュアル登録MACアドレスとして設定されていることを条件としてアクセスを許容する。

【選択図】 図4

特願 2 0 0 3 - 1 3 8 5 5 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

[変更理由]

住 所

氏 名

1 9 9 0 年 8 月 3 0 日

新規登録

東京都品川区北品川 6 丁目 7 番 3 5 号

ソニー株式会社